Extreme networks
ADVANCE WITH US

AirDefense 10.5.0-05a6 Release Notes

AirDefense 10.5.0-05a6 Release Notes

This document is an addendum to the release notes for the main release 10.5.0-05

1. AirDefense 10.5.0-05a6 patch

The AirDefense 10.5.0-05a6 patch is a maintenance release containing customer found bug fixes. The patch also addresses key vulnerabilities reported from our regular scans and customer reported scans.

2. Version Compatibility

Important!	**Only an upgrade from 10.5.0-05 is supported.**

For existing customers who would like to upgrade to 10.5.0-05a6, AirDefense is an entitled product and requires an active support contract.

Firmware Version Compatibility

AirDefense 10.5.0-05a6 has been tested for compatibility against

- WiNG 7.7.1.0
- XCC 05.46.03.0016

Supported Sensor Model and Interop Build version validated

Sensor Model	WING Distributed
AP 7522, AP 7532, AP 7562	WiNG 7.7.1.0
AP 8533	WiNG 7.7.1.0
AP 8432	WiNG 7.7.1.0
AP 310, AP360	WiNG 7.7.1.0
AP 410, AP460	WiNG 7.7.1.0
AP 505, AP 510, AP 560	WiNG 7.7.1.0
AP310-1	WiNG 7.7.1.0
AP410-1	WiNG 7.7.1.0
AP510-1	WiNG 7.7.1.0

Sensor Model	Wing Campus
AP310-1	WiNG 7.8.1.0
AP410-1	WiNG 7.8.1.0
AP510-1	WiNG 7.8.1.0

Sensor Model	IQEngine/HOS
AP410C/AP460C	10.4r3
AP305C	10.4r3

Please see the section titled **DFS Tables, Sensor and Radio Share** in the corresponding WiNG release notes for a detailed matrix of sensor features supported for each access point in that WiNG release.

Hardware Appliances

- Model NX-9500
- Model NX-9600

Virtual Platforms

- VMWare EXSi Hypervisor 5.5, 6.0, and 6.5

3. Installation

Important!	**Only an upgrade from 10.5.0-05 is supported.**

Follow these steps to upgrade an AirDefense system that is currently running AirDefense 10.5.0-05 firmware.

1. Copy the file `AD-upgrade-10.5.0-05a6.tar` file to the **`/usr/local/tmp`** folder on the AirDefense server using the **`smxmgr`** account. You can use transfer protocols such as SCP, SSH, Secure File Transfer Client, or PUTTY.
2. Log in to the AirDefense user interface as **`smxmgr`**. From the menu, select **Software > Servmod** and enter the location of the patch file **`/usr/local/tmp`**.

   The menu now shows the available files.

3. Enter the number corresponding to `AD-upgrade-10.5.0-05a6.tar` and press **Enter**.

   AirDefense installation of the 10.5.0-05a6 patch begins.

For full instructions on how to upload the AirDefense image onto an NX and install it successfully, please see the *Extreme AirDefense Users Guide*.

4. Important Notes

Refer 10.5.0-05 Release notes for more details

5. SPR/Issues Fixed

SPR Number	Title
AD-10461	Duplicate MAC in multicore – Fix is in EQL to remove
AD-11294	Unable to delete security profile even no devices using
AD-11282	Remove vulnerable kexalgorithm diffie-hellman-group1-sha1 from ssh server (Improvement for vulnerability detected in 10.5)
ADIQ-584	Update Postgres time zone setting as well when the system time zone is changed
AD-11268	Check for WIPS license before initiating a termination (APAC IIDA)
ADIQ-623	Comms mgr: ssl error 5 at sensor (Sensor issue fixed – Added AD side recovery)
ADIQ-598	Fix for login issue after the restore.
ADIQ-664	Fix for location in new UI with scaling support change. (Pending verification from QA side with fix build)
ADIQ-665	Adsp Rest API documentation support with swagger
APC-48789	Changes in BSS creation in XIQ, based on received client's BSSID. (XIQ Q3r1 issue)
AD-11304	Whitelisting from XCC controller after termination initiated. (Expire after *X* hours to clear the blacklist from XCC table)
ADIQ-666	APTest Issues
ADIQ-653	Kernel upgrade and other packages for vulnerabilities – fix for new vulnerability reported
AD-11257	Name change issue seen in new generation GUI
AD-11262	Search does not work in auto placement
AD-11244	AirDefense 10.41 location not working if you assign a client type category to a device
AD-11259	Auto logout users while using system
AD-11296	XCC Polling times out
AD-11248	HTML5 UI Action Control Device State Icon Mismatch
AD-11280	Director process crash when export devices from new UI
AD-11272	Failed to delete tree structure using customer configuration

6. Vulnerabilities Fixed

The following packages are updated for the vulnerabilities reported.

- dhcp 4.2.5-83
- glib2 2.56.1-9
- java-1.8.0-openjdk 1.8.0.312.b07-1
- kernel 3.10.0-1160.49.1
- libX11 1.6.7-4

- libxml2 2.9.1-6
- microcode_ctl 2.1-73.11
- nspr 4.32.0
- nss 3.67.0-4
- openssh 7.4p1-22
- openssl .0.2k-22
- postgresql 9.2.24-7

7. Known Issues and Recommendations

General Note

- The Bluetooth icon is seen on AP310-1/AP410-1/AP510-1 when the sensor is connected. However, there is no Bluetooth support on these devices. This is due to an AP side issue while publishing the capabilities.
- AP310-1 will always be reported as AP310i-1 after polling. If the sensor is pointed to an AD server, it reports either AP310e-1 or AP310i-1. Once you enable the SNMP polling on that AP, it will report only as AP310i-1. This is due to the AP side limitation on the system model that is defined.